FIREWALLS

Realizado por:
Jesús Ángel Pérez-Roca Fernández
José Antonio Pereira Suárez

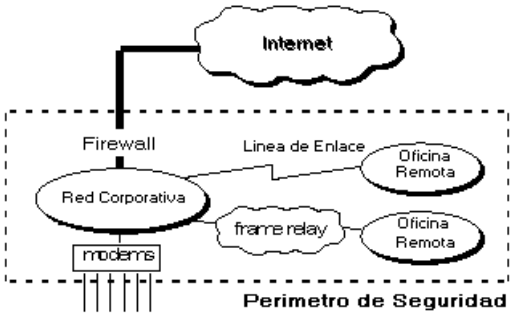
ÍNDICE

Introducción....3
Ventajas de los firewalls....4
Limitaciones de los firewalls....5
Tipos de firewalls....6
  Firewalls hardware....6
  Firewalls software....7
Principales tecnologías para los firewalls hardware....8
  Filtrado de paquetes....8
  De nivel de aplicación....8
  Firewalls híbridos....9
  Firewalls de nivel de aplicación de segunda generación....10
Ataques e intrusiones....10
Política de seguridad en la red....11
Configuración de un firewall en Linux con iptables....12
  ¿Qué es iptables?....12
  Características del firewall a crear....13
  Uso básico de iptables....13
  Creación del firewall....14
  Guardar y reusar nuestra configuración de iptables....16
Windows Firewall....18
  El firewall de Windows....18
  Cómo funciona....18
  Qué hace y qué no hace....19
  Configuración del Firewall....19
  Excepciones....20
  Otras configuraciones....25
Cómo configurar Zone Alarm....27
  Introducción....27
  Configuración de Zone Alarm....28
    Overview....29
    Firewall....30
    Program Control....32
    Alerts & Logs....32
    E-Mail Protection....33
  Observaciones....33
Conclusiones....34
Bibliografía....35

Introducción

La seguridad ha sido el principal tema a tratar cuando una organización desea conectar su red privada a Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el numero de usuarios de redes privadas por la demanda del acceso a los servicios de Internet, tal es el caso del World Wide Web (WWW), Internet Mail (e-mail), Telnet, y File Transfer Protocol (FTP).

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de sus redes a los "usuarios malintencionados". Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información. Aunque una organización no esté conectada a Internet, ésta debería establecer una política de seguridad interna para administrar el acceso de usuarios a partes de la red y proteger sensiblemente la información privada.



Un firewall es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

También es frecuente conectar al firewall una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Si está correctamente configurado, un firewall añade protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

También puede ofrecer control de acceso a los sistemas de un sitio. Por ejemplo, algunos servidores pueden ponerse al alcance de redes externas, mientras que otros pueden cerrarse de una manera efectiva al acceso no deseado.

Un firewall para una organización en que la mayoría del software modificado y el software de seguridad adicional puede localizarse en el sistema de firewall puede resultar menos costoso que si se distribuye en cada servidor o máquina. En particular, los sistemas de contraseña desechables y otro software de autenticación agregado puede localizarse en el firewall en lugar de en cada sistema al cual se necesita tener acceso desde Internet.

También hay que tener en cuenta la seguridad interna. Frecuentemente se da mucho énfasis a un firewall, pero si un hacker irrumpe en un sistema, a menos que éste tenga algunas políticas de seguridad interna en funcionamiento, la red quede expuesta. Por esta razón, muchas veces podría ser buena idea poner el servidor a disposición de internet fuera del firewall. Es muy probable que los servicios queden expuestos a las amenazas de Internet, pero se podría tener fácilmente una réplica del servidor dentro del firewall y que estuviera disponible para una recuperación rápida. También se podría mantener toda la configuración del sistema del servidor externo en un dispositivo de almacenamiento volviéndolo así seguro contra modificaciones.

La privacidad debe ser una gran preocupación para toda red corporativa, debido a que lo que normalmente se consideraría información inocua en realidad podría contener pistas útiles para un hacker. Otra ventaja es que, al pasar a través de un firewall todo el acceso hacia y desde Internet, se puede llevar un registro de los accesos y proporcionar estadísticas valiosas sobre el uso de la red.

Ventajas de los firewalls

Los firewalls en Internet administran los accesos posibles de Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la dureza con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "choke point" (embudo), manteniendo al margen los usuarios no autorizados (hackers, crakers, espías, etc.) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, ya que se consolida la seguridad en el sistema firewall, lo que es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

El firewall ofrece un punto donde la seguridad puede ser monitorizada y si aparece alguna actividad sospechosa, éste generará una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto es muy importante de cara a que el administrador audite y lleve un registro del tráfico significativo a través del firewall. También es importante que el administrador de la red responda a las alarmas y examine regularmente los registros de base.

Un firewall es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT) esto puede ayudar aliviando el espacio de direccionamiento, acortando y eliminando lo necesario para reenumerar cuando la organización cambie de Proveedor de Servicios de Internet (ISP).

Un firewall de Internet es el punto perfecto para auditar o registrar el uso de Internet. Esto permite al administrador de red justificar el gasto que implica la conexión a Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

También ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.

La preocupación principal del administrador de red, son los múltiples accesos a Internet, que se pueden registrar con un monitor y un firewall en cada punto de acceso que posee la organización hacia el Internet. Estos dos puntos de acceso significan dos puntos potenciales de ataque a la red interna que tendrán que ser monitorizados regularmente.

Limitaciones de los firewalls

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

Por ejemplo, si existe una conexión sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una conexión SLIP o PPP al Internet. Los usuarios suelen irritarse cuando se requiere una autenticación adicional requerida por un Firewall Proxy Server (FPS), lo cual puede ser provocado por un sistema de seguridad que esta incluido en una conexión directa SLIP o PPP del ISP.

El firewall no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El firewall no puede prohibir que los traidores o espías corporativos copien datos privados en dispositivos de almacenamiento externo y substraigan los datos del edificio.

El firewall no puede proteger contra los ataques de la Ingeniería Social, por ejemplo, un hacker que pretende ser un supervisor o un nuevo empleado despistado, persuade al menos sofisticado de los usuarios a que le permita usar su contraseña al servidor del corporativo o que le permita el acceso temporal a la red.

El firewall no puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. El firewall no puede contar con un sistema preciso de escaneado para cada tipo de virus que se puedan presentar en los archivos que pasan a través de el.

La solución real está en que la organización debe instalar software antivirus en cada despacho para protegerse de los virus que llegan ya sea por Internet o por cualquier dispositivo físico.

Finalmente, el firewall no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno y son ejecutados creando un ataque. Por ejemplo, una transferencia de datos podría causar que un servidor modificara los archivos relacionados a la seguridad haciendo más fácil el acceso de un intruso al sistema.

Tipos de firewalls

Los Firewall tradicionales son de hardware, es decir, un dispositivo específico instalado en una red para levantar una defensa y proteger a la red del exterior. Son utilizados en entornos profesionales: el administrador de red define una serie de reglas para permitir el acceso y detiene los intentos de conexión no permitidos.

Los Firewall personales son programas que filtran el tráfico que entra y sale de una computadora. Una vez instalados, el usuario debe definir el nivel de seguridad: permite o deniega el acceso de determinados programas a Internet (de forma temporal o definitiva) y autoriza o no los accesos desde el exterior.

Firewalls hardware

Los firewall de hardware se utilizan más en empresas y grandes corporaciones. Normalmente son dispositivos que se colocan entre el router y la conexión telefónica. Como ventajas, podemos destacar que al ser independientes del PC, no es necesario configurarlos cada vez que reinstalamos el sistema operativo y no consumen recursos del sistema.

Su mayor inconveniente es el mantenimiento, ya que son difíciles de actualizar y de configurar correctamente.

Los firewalls hardware pueden ser adquiridos como un producto independiente pero recientemente los firewalls hardware suelen encontrarse integrados en routers de banda ancha y deberían ser considerados una parte importante de cara a la configuración de una red, especialmente cuando se usa una conexión de banda ancha. Los firewalls hardware pueden ser efectivos con muy poca o ninguna configuración previa y pueden proteger todas las máquinas de una red local. La mayoría tienen como mínimo cuatro puertos para conectarse a otras máquinas, pero para redes más grandes existen otras soluciones de negocio.

Los firewalls hardware usan filtrado de paquetes para examinar la cabecera de un paquete y así determinar su origen y su destino. Esta información se compara con un conjunto de reglas predefinidas o creadas por el usuario que determinan si el paquete tiene que ser redirigido o descartado.

Como con cualquier otro dispositivo electrónico, un usuario con conocimientos generales sobre informática puede conectar un firewall, ajustar unas cuantas opciones y ponerlo a funcionar. De todas formas, para asegurarse de que un firewall está configurado para una protección y seguridad óptimas, podría ser necesario aprender las características específicas del modelo de firewall instalado, cómo activarlas y cómo probar el firewall para asegurarse de que está protegiendo la red de forma correcta.

No todos los firewalls son iguales, por lo que es muy importante leer el manual de instrucciones y toda la documentación que viene con el producto. Adicionalmente, la página web del fabricante puede tener también cierta información interesante de cara al usuario primerizo.

Para probar el nivel de seguridad de un firewall hardware, se pueden usar herramientas de terceros o buscar en Internet un servicio gratuito de prueba de firewalls online. La prueba del firewall es una parte muy importante del mantenimiento, ya que sirve para saber si el firewall está bien configurado y la protección que nos ofrece es óptima.

Entre los principales fabricantes de firewalls hardware destacan Checkpoint y Cisco.

Firewalls software

Estos programas son los más comunes en los hogares, ya que, a parte de resultar mucho más económicos que el hardware, su instalación y actualización es más sencilla. Eso sí, presentan algunos problemas inherentes a su condición: consumen recursos del PC, algunas veces no se ejecutan correctamente o pueden ocasionar errores de compatibilidad con otro software instalado.

Actualmente, los sistemas operativos más modernos como Windows XP y Linux integran soluciones básicas de firewall , en algunos casos, como en el software libre, son muy potentes y flexibles, pero requieren un gran conocimiento en redes y puertos necesarios para las aplicaciones. Para no tener problemas, existen una serie de herramientas externas que facilitan este trabajo de protección.

Para los usuarios “normales”, la mejor opción de firewalls es un firewall software. Los firewalls software se instalan en el ordenador (como cualquier otro programa) y pueden ser configurados de diversas maneras, permitiendo cierto control sobre su funcionalidad y sus características de protección. Los firewalls software protegen el ordenador ante ataques externos que intentan obtener el control de la máquina o conseguir acceso a la misma y, dependiendo del programa de firewall, puede también proporcionar protección contra los virus, troyanos y gusanos más comunes. Muchos firewalls software tienen controles definidos por el usuario para establecer una compartición segura de archivos e impresoras y para bloquear aplicaciones no seguras e impedir que se ejecuten en el sistema. Adicionalmente, los firewalls software pueden incorporar también controles de privacidad, filtrado de webs y mucho más. Lo malo que tiene este tipos de firewalls es que, al contrario de lo que ocurre con los firewalls harware, los firewalls software sólo protegen el ordenador en el que están instalados y no protegen la red entera, así que cada ordenador necesitará tener instalado el firewall software.

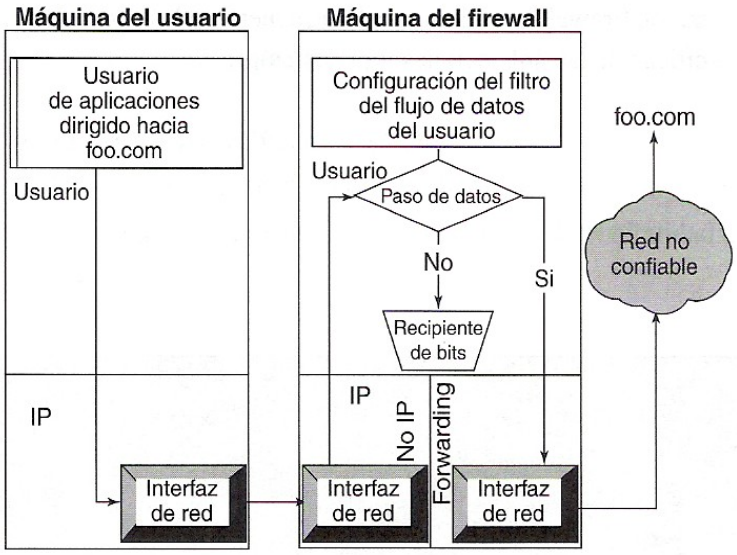
Al igual que ocurre con los firewalls hardware, hay un gran número de firewalls software en el mercado. Debido a que el firewall software debe estar siempre ejecutándose en cada ordenador, debería tenerse en cuenta los recursos que necesita para ejecutarse y también es importante comprobar que no haya ninguna incompatibilidad de cara a la elección del firewall software. Un buen firewall software se ejecutará en segundo plano en el sistema y usará sólo una pequeña parte de los recursos del mismo. Es importante monitorizar el firewall software una vez instalado y descargar e instalar las actualizaciones disponibles periódicamente.

Las diferencias entre los dos tipos de firewalls son amplias y la mejor protección para una red es utilizar los dos, ya que cada uno ofrece características de seguridad diferentes. Actualizar el firewall y el sistema operativo es esencial para mantener una protección optima, así como comprobar que el firewall está conectado y funcionando correctamente.

Principales tecnologías para los firewalls hardware

Filtrado de paquetes

Este tipo de firewall proporciona control de acceso en el nivel IP y acepta o rechaza los paquetes basándose en el origen, en las direcciones de la red de destino y en tipo de aplicaciones. Los firewalls de filtrado de paquetes proporcionan un nivel de seguridad muy simple por un precio relativamente económico. Este tipo de firewalls, por lo general, son transparentes para los usuarios.



Firewall de gateway de aplicación (Socks)

Debilidades:

1. Son vulnerables ante los ataques dirigidos a protocolos superiores a los del protocolo del nivel de red, ya que éste es el único nivel que comprenden.
2. Debido a que el protocolo de nivel de red requiere ciertos conocimientos acerca de sus detalles técnicos y que no todos los administradores cuentan con ellos, los firewalls de filtrado de paquetes son, por lo general, más difíciles de configurar y de verificar, lo cual incrementa los riesgos de tener sistemas con configuraciones erróneas, agujeros en la seguridad y fallas.
3. No pueden ocultar la topología de red privada y por lo tanto exponen a la red privada al mundo exterior.
4. No todas las aplicaciones de Internet están soportadas por los firewalls de filtrado de paquetes.
5. Estos firewalls no siempre soportan algunas de las cláusulas de las políticas de seguridad, como la autenticación de nivel de usuario y el control de acceso por hora del día.

De nivel de aplicación

Este tipo de firewalls proporcionan control de acceso en el nivel de aplicación. Por lo tanto, actúa como una puerta de enlace al nivel de aplicación entre dos redes. Debido a que estos firewalls funcionan en este mismo nivel, tienen la capacidad de examinar el tráfico con detalle, lo cual hace que sean más seguros que los firewalls de filtrado de paquetes. Además, este tipo de firewall generalmente es más lento que el de filtrado de paquetes debido al examen riguroso del tráfico. Por

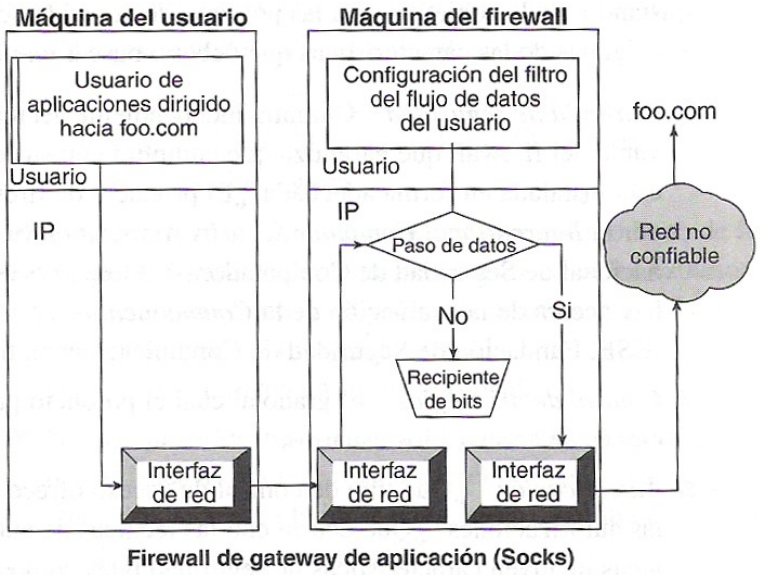
lo tanto, hasta cierto grado son molestos, restrictivos y comúnmente requieren que los usuarios cambien su comportamiento o que utilicen un software especial con el fin de lograr los objetivos de las políticas. Por este motivo, los firewalls de nivel de aplicación no son transparentes para los usuarios.

Ventajas:

1. Debido a que entienden al protocolo de nivel de aplicación pueden defenderse en contra de todos los ataques.
2. Por lo general son mucho más fáciles de configurar debido a que no requieren que se conozcan todos los detalles acerca de los protocolos de los niveles más bajos.
3. Pueden ocultar la topología de la red privada.
4. Pueden soportar más políticas de seguridad incluyendo la autenticación de nivel de usuario y el control de acceso de hora del día.

Firewalls híbridos

Conscientes de las debilidades de los firewalls de filtrado de paquetes y de los de nivel de aplicación, algunos proveedores han introducido firewalls híbridos que combinan las técnicas de los otros dos tipos. Aunque estos productos híbridos intentan resolver algunas de las debilidades anteriormente mencionadas, introducen varias debilidades inherentes en los firewalls de nivel de aplicación como las que se describieron en la lista anterior.



Debilidad: Debido a que los firewalls híbridos siguen basándose en los mecanismos de filtrado de paquetes para soportar ciertas aplicaciones, aún tienen las mismas debilidades en la seguridad.

Firewalls de nivel de aplicación de segunda generación

Este tipo de firewalls continúa siendo un firewall de nivel de aplicación, pero se encuentra en su segunda generación, la cual resuelve el problema de la transferencia que se presentaba en las versiones anteriores sin sacrificar el desempeño.

Ventajas:

1. Pueden utilizarse como un firewall de intranet debido a su transparencia y a que su desempeño general es mayor.
2. Pueden proporcionar una completa traducción de direcciones de red además de que ocultan la topología de la red.
3. Soportan más mecanismos avanzados de autenticación de nivel de usuario.

Ataques e intrusiones

Podemos definir como ataques, todas aquellas acciones que suponen una violación de la seguridad de nuestro sistema, confidencialidad, integridad o disponibilidad.

Estas acciones se pueden clasificar de modo genérico según los efectos causados, como:

- **Interrupción:** cuando un recurso del sistema es destruido o se vuelve no disponible.
- **Intercepción:** una entidad no autorizada consigue acceso a un recurso.
- **Modificación:** alguien no autorizado consigue acceso a una información y es capaz de manipularla.
- **Fabricación:** cuando se insertan objetos falsificados en el sistema.

También se pueden ordenar por modalidades de ataque según la forma de actuar:

- **Escaneo de puertos:** esta técnica consiste en buscar puertos abiertos, y fijarse en los que puedan ser receptivos o de utilidad.
- **Ataques de autentificación:** cuando un atacante suplanta a una persona con autorización.
- **Explotación de errores:** suceden en el momento que se encuentran agujeros de seguridad en los sistemas operativos, protocolos de red o aplicaciones.
- **Ataques de denegación de servicio (DoS):** consiste en saturar un servidor con pedidos falsos hasta dejarlo fuera de servicio.

Consejos para defenderse de este tipo de ataques:

- Mantener el sistema operativo y las aplicaciones actualizadas.
- Un buen firewall con el que evitaremos el escaneo de puertos y el acceso no autorizado a nuestro ordenador.
- Un antivirus que apoye el trabajo del firewall.
- Cambiar las contraseñas que viene por defecto en el sistema operativo.
- Poner especial cuidado a la hora de compartir archivos y recursos.

Política de seguridad en la red

La decisión de instalar un firewall puede estar influenciada por dos niveles de política de red: instalación y uso del sistema. La política de acceso a la red que define los servicios que se permitirán o negarán de manera explícita desde la red restringida es la política de más alto nivel. También define cómo se utilizarán estos servicios. La política de más bajo nivel define cómo se restringirá en realidad el acceso y determinará los servicios especificados en la política de nivel superior. Sin embargo, una política no debe volverse un documento aislado sino que debe ser útil. Es imprescindible que la política de seguridad de red se vuelva parte de la política de seguridad de la compañía.

Una política de seguridad es muy importante al instalar un firewall en una compañía, debido a que señala cuáles son los valores que vale la pena proteger y cuáles son las acciones o procedimientos para la administración de riesgos que se deben seguir con el fin de proteger los valores corporativos.

Con frecuencia, las políticas de seguridad de red integran aspectos de seguridad de políticas anteriores. Por lo general, las compañías buscan asistencia externa cuando configuran por primera vez la política de seguridad de su red.

Hay dos políticas básicas en la configuración de un cortafuegos y que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- **Política restrictiva**: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.
- **Política permisiva**: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico

potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

Configuración de un firewall en Linux con iptables

¿Qué es iptables?

`iptables` es la herramienta que nos permite configurar las reglas del sistema de filtrado de paquetes del kernel de Linux, desde su versión 2.4 (en 2.2 era ipchains). Con esta herramienta, podremos crearnos un firewall adaptado a nuestras necesidades.

Su funcionamiento es simple: a iptables se le proporcionan unas ***reglas***, especificando cada una de ellas unas determinadas características que debe cumplir un paquete. Además, se especifica para esa regla una ***acción*** o ***target***. Las reglas tienen un orden, y cuando se recibe o se envía un paquete, las reglas se recorren en orden hasta que las condiciones que pide una de ellas se cumplen en el paquete, y la regla se activa realizando sobre el paquete la acción que le haya sido especificada.

Estas acciones se plasman en los que se denominan ***targets***, que indican lo que se debe hacer con el paquete. Los más usados son bastante explícitos: **ACCEPT**, **DROP** y **REJECT**, pero también hay otros que nos permiten funcionalidades añadidas y algunas veces interesantes: **LOG**, **MIRROR**...

En cuanto a los paquetes, el total del sistema de filtrado de paquetes del kernel se divide en tres *tablas*, cada una con varias ***chains*** a las que puede *pertenecer* un paquete, de la siguiente manera.

- **filter**: Tabla por defecto, para los paquetes que se refieran a nuestra máquina.
  - **INPUT**: Paquetes recibidos para nuestro sistema.
  - **FORWARD**: Paquetes enrutados a través de nuestro sistema.
  - **OUTPUT**: Paquetes generados en nuestro sistema y que son enviados.
- **nat**: Tabla referida a los paquetes enrutados en un sistema con Masquerading.
  - **PREROUTING**: Para alterar los paquetes según entren.
  - **OUTPUT**: Para alterar paquetes generados localmente antes de enrutar.
  - **POSTROUTING**: Para alterar los paquetes cuando están a punto para salir.
- **mangle**: Alteraciones más *especiales* de paquetes.
  - **PREROUTING**: Para alterar los paquetes entrantes antes de enrutar.
  - **OUTPUT**: Para alterar los paquetes generados localmente antes de enrutar.

Dado que el soporte para el firewall está integrado en el kernel de Linux (**Netfilter**), para poder usar iptables tendremos que asegurarnos de que nuestro núcleo admite el uso de `iptables` y que añadimos a la configuración del núcleo todos aquellos *targets* que vayamos a necesitar (aunque siempre es bueno tener los más posibles).

Características del firewall a crear

Para crear nuestro sencillo firewall doméstico, tendremos primero que preguntarnos qué es lo que deseamos que haga. Lo más usual, en un equipo que se usa para conexiones a Internet de manera normal (no es servidor de nada, etc...) es que deseemos de nuestro firewall lo siguiente:

- Que **permita realizar conexiones TCP** hacia afuera de nuestra máquina (si no, no podríamos hacer casi nada).
- Que **no permita realizar conexiones TCP desde afuera hacia nuestra máquina**, para evitar que alguien intente conectarse a nuestros servidores web, ftp, telnet, X...
- Que **permita el tráfico de paquetes TCP (paquetes que no establezcan conexiones) en ambas direcciones**, pues necesitamos tráfico bidireccional de paquetes al usar casi cualquier cosa en Internet.
- Que **prohiba el tráfico UDP desde afuera de nuestra máquina**, a excepción del necesario para las respuestas por parte de nuestros servidores **DNS**, que provendrán de su puerto UDP 53.
- En caso de tener una intranet, que **no aplique estas restricciones al tráfico proveniente de y enviado hacia la intranet**, ya que en esta red interna probablemente sí nos interese poder acceder remotamente a nuestra máquina.

Uso básico de iptables

Para crear nuestro firewall, necesitaremos ejecutar algunos comandos básicos sobre `iptables`:

- Para crear una nueva regla al final de las ya existentes en una *chain* determinada:

```
$ /sbin/iptables -A [chain] [especificacion_de_la_regla]
[opciones]
```

- Para insertar una regla en una posición determinada de la lista de reglas de una *chain* determinada:

```
$ /sbin/iptables -I [chain] [posición]
```

```
[especificacion_de_la_regla] [opciones]
```

- Para borrar una regla en una posición determinada de la lista de reglas de una *chain* determinada:

```
$ /sbin/iptables -D [chain] [posición]
```

- Para todas las reglas de una *chain* determinada:

```
$ /sbin/iptables -F [chain]
```

- Para listar las reglas de una *chain* determinada:

```
$ /sbin/iptables -L [chain]
```

La **especificación de reglas** se hace con los siguientes parámetros (especificando aquellos que se necesite):

- **-p [protocolo]**: Protocolo al que pertenece el paquete.
- **-s [origen]**: Dirección de origen del paquete, puede ser un nombre de host, una dirección IP normal, o una dirección de red (con máscara, de forma dirección/máscara).
- **-d [destino]**: Al igual que el anterior, puede ser un nombre de host, dirección de red o dirección IP singular.
- **-i [interfaz-entrada]**: Especificación del interfaz por el que se recibe el paquete.
- **-o [interfaz-salida]**: Interfaz por el que se va a enviar el paquete.
- **[!] -f**: Especifica que la regla se refiere al segundo y siguientes fragmentos de un paquete fragmentado. Si se antepone !, se refiere sólo al primer paquete, o a los paquetes no fragmentados.
- **`-j [target]`**: Nos permite elegir el target al que se debe enviar ese paquete, esto es, la acción a llevar a cabo con él.

Algunas de las opciones que se permiten en los comandos de arriba son:

- **-v**: Modo *verboso*, útil sobre todo con iptables -L.
- **-n**: las direcciones IP y números de puertos se mostrarán numéricamente (sin resolver nombres).
- **--line-numbers**: Muestra los número de regla de cada regla, de manera que sea más fácil identificarlas para realizar operaciones de inserción, borrado...

Creación del firewall

Para crear nuestro firewall, iremos introduciendo una a una las reglas que necesitamos:

Primera regla: **permitiremos cualquier tráfico que provenga de nuestro interfaz de loopback (lo)**, para ello insertaremos en el *chain* INPUT (que se encarga de los paquetes que llegan con destino a nuestra máquina), de la tabla **filter** la siguiente regla:

```
$ /sbin/iptables -A INPUT -i lo -j ACCEPT
```

Atención: es importante aquí **respetar las mayúsculas**, pues los nombres del *chain* y del target son **INPUT** y **ACCEPT**, no **input** o **accept**.

Segunda regla: **si disponemos de intranet, permitiremos todo el tráfico que provenga de nuestro interfaz de red interna**. Por ejemplo, imaginando que tuviésemos una ethernet en el interfaz `eth0`, haríamos:

```
$ /sbin/iptables -A INPUT -i eth0 -j ACCEPT
```

El hecho de que omitamos la dirección de origen, de destino... implica que nos referimos a **todas**.

Tercera regla: **impediremos el paso de cualquier paquete TCP proviniente del exterior que intente establecer una conexión con nuestro equipo**. Estos paquetes se reconocen por tener el flag SYN asertado y los flags ACK y FIN desasertados. Para decirle a la regla que reconozca específicamente estos paquetes, usaremos una opción que se puede usar cuando el protocolo del paquete es declarado como **tcp**, la opción **--syn**. De la siguiente manera:

```
$ /sbin/iptables -A INPUT -p tcp --syn -j REJECT --reject-with
icmp-port-unreachable
```

Y vemos también el uso de una opción del target **REJECT**, que nos permite elegir de qué manera debe ser rechazado el paquete. Posibles valores son **icmp-net-unreachable**, **icmp-host-unreachable**, **icmp-port-unreachable**, **icmp-proto-unreachable**, **icmp-net-prohibited** y **icmp-host-prohibited**.

Cuarta regla: Antes de declarar que deseamos prohibir cualquier tráfico UDP hacia nuestra máquina, y dado que las reglas se recorren en orden hasta que una de ellas se activa con el paquete, **tendremos que añadir ahora una regla que nos permita recibir las respuestas de nuestro/s servidor/es DNS** cuando nuestro sistema les realice alguna consulta. Estas respuestas, vía UDP, saldrán del puerto 53 del servidor DNS. La regla, pues, será:

```
$ /sbin/iptables -A INPUT -p udp --source-port 53 -j ACCEPT
```

Donde **--source-port** es una opción presente cuando el protocolo es **udp** (también cuando es **tcp**) y nos permite en este caso especificar que la consulta provenga del puerto destinado al DNS.

Quinta regla: **Prohibimos ahora el resto del tráfico UDP**. La regla de por sí implica a todo el tráfico UDP, pero como un paquete sólo activará esta regla si no ha activado la anterior, los paquetes UDP referentes a una transacción con un servidor de nombres no se verán afectados.

```
$ /sbin/iptables -A INPUT -p udp -j REJECT --reject-with icmp-
port-unreachable
```

Dado que los targets por defecto (**denominados *policy* o política**) en la tabla filter son ACCEPT, si un paquete no activa ninguna de las reglas, será aceptado, de manera que no tendremos que preocuparnos de, por ejemplo, los paquetes de tráfico normal de TCP, ya que estos serán aceptados al no activar regla alguna.

Si ahora escribimos:

```
$ /sbin/iptables -L -v
```

Deberíamos obtener algo como:

```
Chain INPUT (policy ACCEPT 3444 packets, 1549K bytes)
pkts bytes target prot opt in out source destination
11312 3413K ACCEPT all -- lo any anywhere anywhere
0 0 ACCEPT all -- eth0 any anywhere anywhere
0 0 REJECT tcp -- any any anywhere anywhere tcp
flags:SYN,RST,ACK/SYN reject-with icmp-port-unreachable
0 0 ACCEPT udp -- any any anywhere anywhere udp spt:domain
0 0 REJECT udp -- any any anywhere anywhere reject-with icmp-
port-unreachable

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 15046 packets, 4218K bytes)
pkts bytes target prot opt in out source destination
```

De modo que nuestro pequeño y básico firewall doméstico ya está configurado. Nuestro equipo es ahora muchísimo más seguro, puesto que los ataques a nuestro sistema requerirían ahora mucha más elaboración, tiempo y esfuerzo por parte del atacante, de manera que nuestra condición de *insignificantes* ya empezará a ser importante como garante de seguridad.

Guardar y reusar nuestra configuración de iptables

Pero, si una vez realizadas estas configuraciones, apagásemos nuestro equipo, todo esto se perdería, y tendríamos que volver a realizar una a una las sentencias de configuración.

Para evitar esto, iptables cuenta con dos programas auxiliares: iptables-save e iptables-restore, el primero de los cuales nos permite sacar por salida estándar el contenido de nuestras tablas IP, y el segundo nos permite, a partir de la salida generada por iptables-save, recuperar la configuración de las tablas.

De manera que para volcar la configuración de nuestro firewall en un fichero ejecutaremos:

```
$ /sbin/iptables-save -c > [fichero]
```

Donde **-c** es una opción que nos permite guardar los contadores del número de paquetes que activaron cada regla.

Y, cuando queramos, podremos recuperar la configuración del firewall con:

```
$ /sbin/iptables-restore -c < [fichero]
```

En cuyo caso **-c** tiene el mismo significado que con `iptables-save`

Estas llamadas a `iptables-save` e `ipatbles-restore` podrán ser incluidas en los scripts adecuados para que se lleven a cabo de manera automática en el arranque y el cierre del sistema.

En caso de ser usuarios de Red Hat Linux, a partir de su versión 7.1, una vez configurado el firewall con `iptables` tal y como se ha descrito en este artículo, y una vez salvada la configuración con `iptables-save` en el archivo **`/etc/sysconfig/iptables`**, se pueden activar los scripts que arrancarán y cerrarán el firewall automáticamente al arrancar y apagar el equipo, mediante la **Text Mode Setup Utility** (**/usr/sbin/setup**), en la sección **System Services**.

Windows Firewall

El firewall de Windows

El sistema operativo Windows XP con Service Pack 2 (SP2), incluye un Firewall, llamado hasta ahora Servidor de seguridad de conexión a Internet o ICF, que está activado de forma predeterminada. Esto significa que la mayor parte de los programas no podrán aceptar comunicaciones de Internet que no hayan solicitado a menos que decida catalogarlos como excepciones. Hay dos programas que, de manera predeterminada, se agregan a la lista de excepciones y pueden aceptar comunicaciones no solicitadas de Internet: Asistente para transferencia de archivos y configuraciones y Compartir impresoras y archivos.

Puesto que los servidores de seguridad restringen la comunicación entre el equipo e Internet, es posible que tenga que ajustar la configuración de algunos programas que funcionan mejor con una conexión abierta. Puede hacer una excepción con estos programas, de modo que se puedan comunicar a través de Firewall de Windows.

Para abrir Firewall de Windows

1. Haga clic en **Inicio** y, a continuación, haga clic en **Panel de control**.
2. En el Panel de control, haga clic en **Centro de seguridad de Windows**.

3. Haga clic en **Firewall de Windows**.

Cómo funciona

Cuando alguien en Internet o en una red intenta conectarse a un equipo, ese intento se conoce como “solicitud no solicitada”. Cuando el equipo recibe una solicitud no solicitada, Firewall de Windows bloquea la conexión. Si utiliza un programa, por ejemplo, de mensajería instantánea o un juego de red con varios jugadores, que tiene que recibir información desde Internet o de una red, el servidor de seguridad le pregunta si desea bloquear o desbloquear (permitir) la conexión. Verá una ventana como la que se muestra a continuación.

Windows Security Alert
To help protect your computer, Windows Firewall has blocked some features of this program.
Do you want to keep blocking this program?
Name: AOL Instant Messenger
Publisher: America Online, Inc.
Keep Blocking
Unblock
Ask Me Later
Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

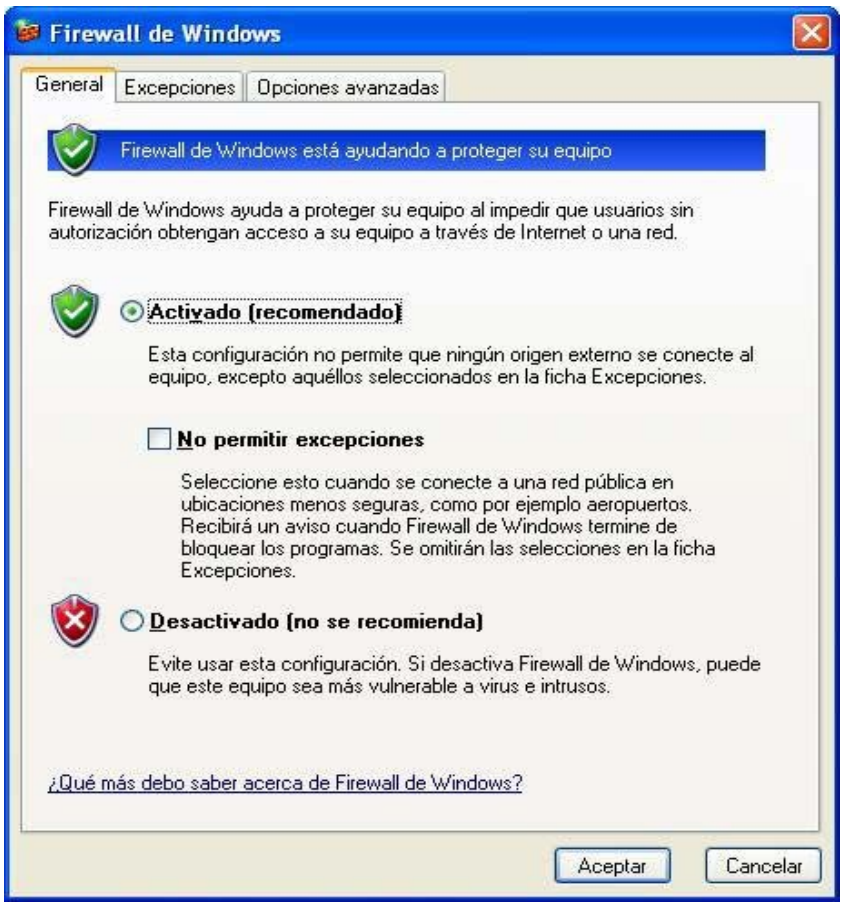
Si elige desbloquear la conexión, Firewall de Windows crea una excepción de modo que el servidor de seguridad no se interpondrá cuando ese programa tenga que recibir información en el futuro.

Qué hace y qué no hace

- **Ayuda a evitar que virus y gusanos informáticos** lleguen a un equipo.
- **Pide el permiso del usuario** para bloquear o desbloquear ciertas solicitudes de conexión.
- **Crea un registro de seguridad**, si desea tener uno, que almacene los intentos correctos y fallidos de conectarse a un equipo. Esto puede ser de utilidad como herramienta de solución de problemas.
- **No detecta o deshabilita los virus y gusanos informáticos** si ya se encuentran en el equipo. Por ese motivo, debería instalar también software antivirus y mantenerlo actualizado para ayudar a impedir que virus, gusanos y otras amenazas para la seguridad dañen el equipo o lo usen para propagarse.
- **No impide que el usuario abra correo electrónico con archivos adjuntos peligrosos**. No abra archivos adjuntos de correo electrónico que provenga de remitentes que no conozca. Incluso aunque conozca y confíe en el origen del mensaje, debe actuar con precaución. Si alguien a quien conoce le envía un archivo adjunto en el correo electrónico, observe la línea de asunto cuidadosamente antes de abrirlo. Si la línea de asunto parece un galimatías o no tiene sentido para usted, consulte al remitente antes de abrirlo.
- **No impide que el correo no solicitado o spam** aparezca en la bandeja de entrada. Sin embargo, algunos programas de correo electrónico pueden servir de ayuda en ese propósito.

Configuración del Firewall

El acceso a la configuración del Firewall también es directamente accesible desde el panel de control, donde podremos encontrar un icono que pone “Firewall de Windows”, que al pulsarlo nos muestra el siguiente cuadro de dialogo:


Firewall de Windows
General
Excepciones
Opciones avanzadas
Firewall de Windows está ayudando a proteger su equipo
Firewall de Windows ayuda a proteger su equipo al impedir que usuarios sin autorización obtengan acceso a su equipo a través de Internet o una red.
Activado (recomendado)
Esta configuración no permite que ningún origen externo se conecte al equipo, excepto aquéllos seleccionados en la ficha Excepciones.
No permitir excepciones
Seleccione esto cuando se conecte a una red pública en ubicaciones menos seguras, como por ejemplo aeropuertos. Recibirá un aviso cuando Firewall de Windows termine de bloquear los programas. Se omitirán las selecciones en la ficha Excepciones.
Desactivado (no se recomienda)
Evite usar esta configuración. Si desactiva Firewall de Windows, puede que este equipo sea más vulnerable a virus e intrusos.
¿Qué más debo saber acerca de Firewall de Windows?
Aceptar
Cancelar

El primer cambio consiste en el modo en el que queremos configurar el Firewall: activado, desactivado o activado sin excepciones. Este último modo resulta de gran utilidad para equipos con movilidad ya que si nos encontramos en un lugar publico podemos, simplemente marcando esta opción, cerrar completamente el acceso al PC en cuestión.

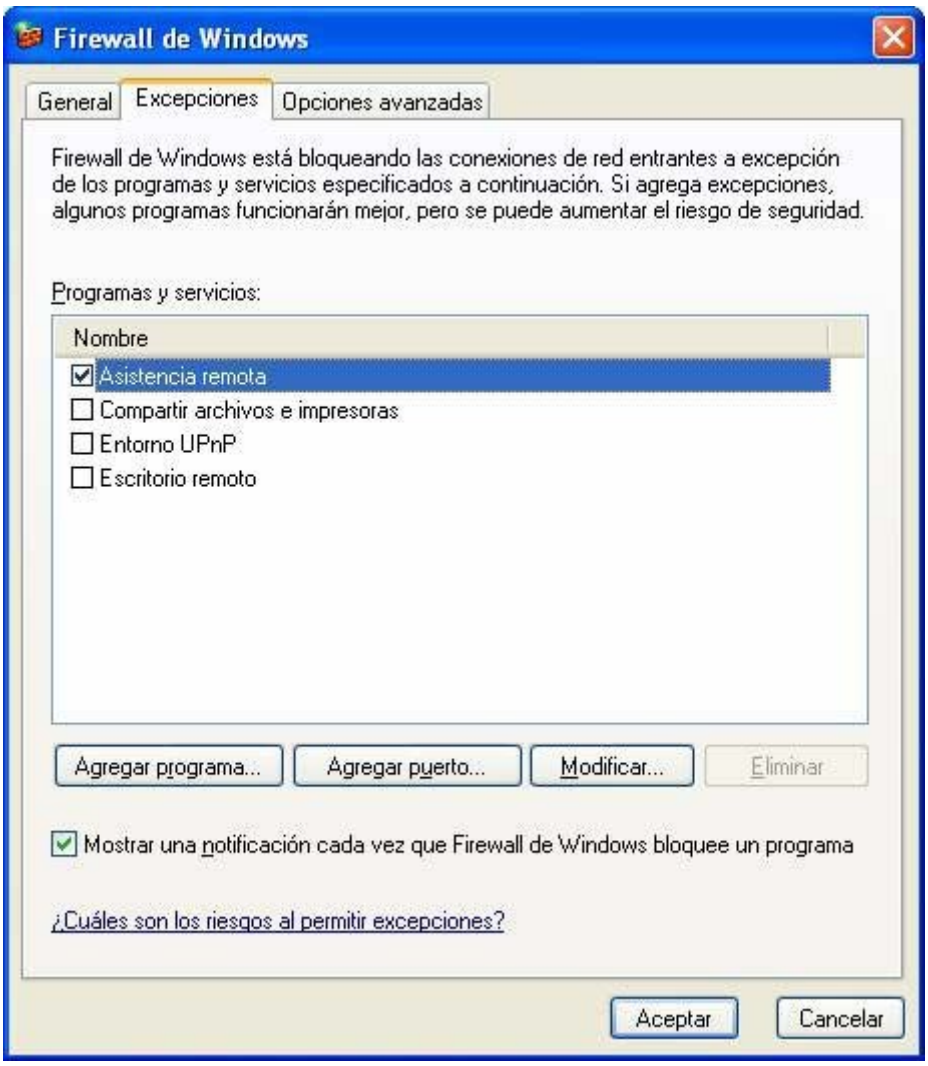
Excepciones

Permitir excepciones tiene ciertos riesgos. Cada vez que permite una excepción para que un programa se comunique a través de Firewall de Windows, el equipo se vuelve más vulnerable. Permitir una excepción es como hacer un agujero en el servidor de seguridad. Si hay demasiados agujeros, no queda mucha pared en el muro que es el servidor de seguridad. Los piratas informáticos suelen usar software que examina Internet en busca de equipos con conexiones sin proteger. Si tiene muchas excepciones y puertos abiertos, el equipo puede ser mucho más vulnerable.

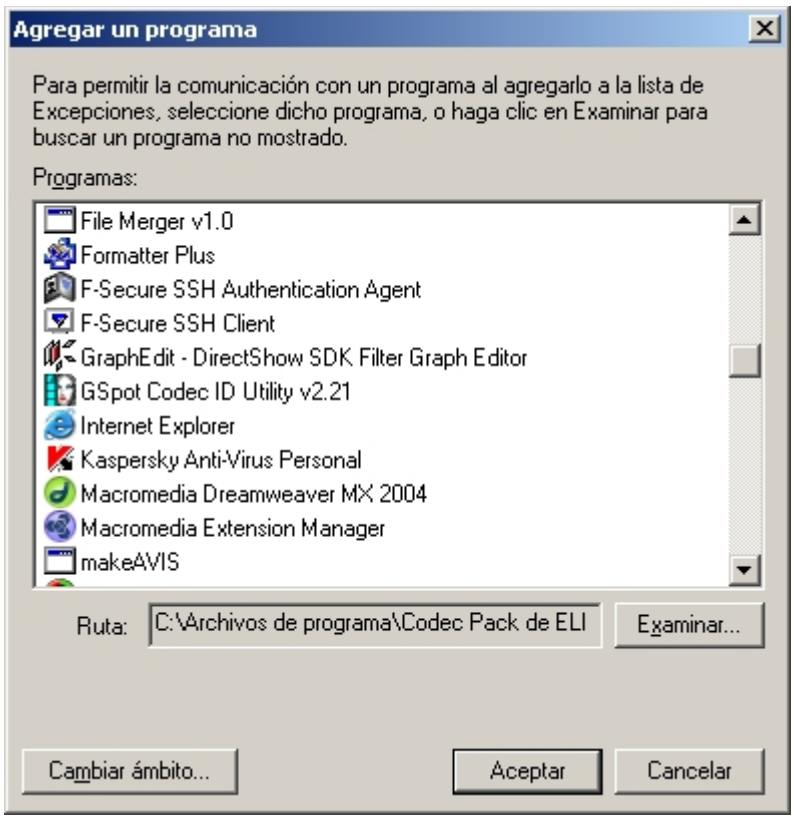
Para contribuir a reducir el riesgo para la seguridad:

- Permita una excepción únicamente cuando la necesite en realidad.
- No permita nunca una excepción para un programa que no reconozca.
- Quite una excepción cuando ya no la necesite

En versiones anteriores esta configuración se debía realizar a mano, con lo que muchos usuarios se veían incapaces de realizarla. Para dar permisos a un programa pulse el botón “Agregar programa...”

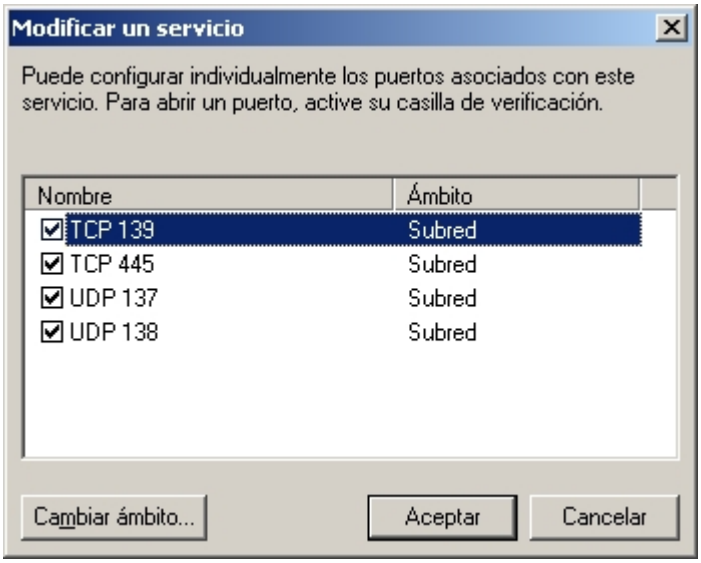

Firewall de Windows
General
Excepciones
Opciones avanzadas
Firewall de Windows está bloqueando las conexiones de red entrantes a excepción de los programas y servicios especificados a continuación. Si agrega excepciones, algunos programas funcionarán mejor, pero se puede aumentar el riesgo de seguridad.
Programas y servicios:
Nombre
Asistencia remota
Compartir archivos e impresoras
Entorno UPnP
Escritorio remoto
Agregar programa...
Agregar puerto...
Modificar...
Eliminar
Mostrar una notificación cada vez que Firewall de Windows bloquee un programa
¿Cuáles son los riesgos al permitir excepciones?
Aceptar
Cancelar

y seleccione el programa que desea añadir:

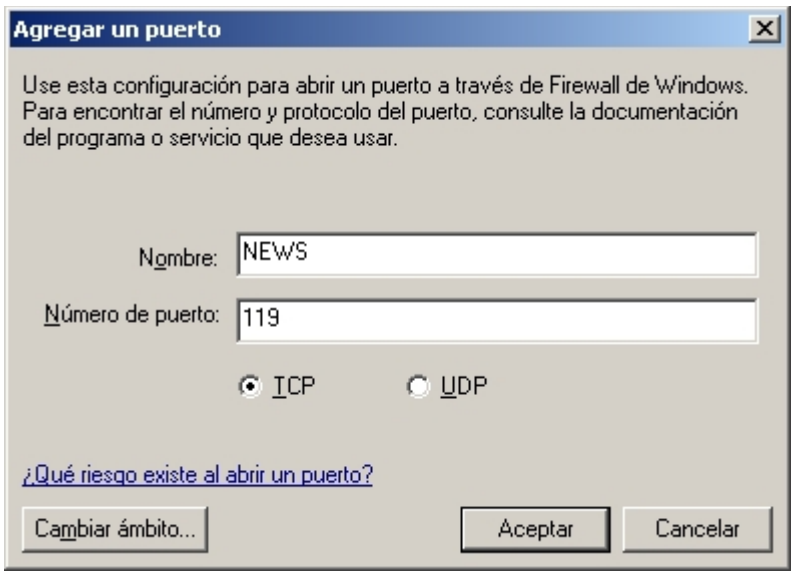

Agregar un programa
Para permitir la comunicación con un programa al agregarlo a la lista de Excepciones, seleccione dicho programa, o haga clic en Examinar para buscar un programa no mostrado.
Programas:
File Merger v1.0
Formatter Plus
F-Secure SSH Authentication Agent
F-Secure SSH Client
GraphEdit - DirectShow SDK Filter Graph Editor
GSpot Codec ID Utility v2.21
Internet Explorer
Kaspersky Anti-Virus Personal
Macromedia Dreamweaver MX 2004
Macromedia Extension Manager
makeAVIS
Ruta:
C:\Archivos de programa\Codec Pack de ELI
Examinar...
Cambiar ámbito...
Aceptar
Cancelar

Si no se encuentra en la lista, puede buscarlo pulsando el boton “Examinar” el cual le abrirá un “Explorador de Archivos” de su PC.

El Firewall detecta automáticamente los puertos que usa el programa seleccionado y los abre cuando ese programa se ejecuta, cerrándolos cuando el programa se cierra. Aunque seleccionando un programa en el cuadro de diálogo de “Excepciones” y pulsando el botón “Modificar” podemos controlar individualmente los puertos que se abren al ejecutar el programa.



Desde la ventana de excepciones también es posible añadir simplemente puertos tanto TCP como UDP, pulsando en el botón 'Agregar puerto...'.


Agregar un puerto
Use esta configuración para abrir un puerto a través de Firewall de Windows. Para encontrar el número y protocolo del puerto, consulte la documentación del programa o servicio que desea usar.
Nombre:
NEWS
Número de puerto:
119
TCP
UDP
¿Qué riesgo existe al abrir un puerto?
Cambiar ámbito...
Aceptar
Cancelar

Otra de las configuraciones de este apartado es el rango de direcciones IP al que vamos a permitir el acceso. Se dividen en tres tipos: las de mi red (Intranet o red interna, técnicamente la misma subred), cualquiera, o un rango definido a mano en una lista de direcciones IP.

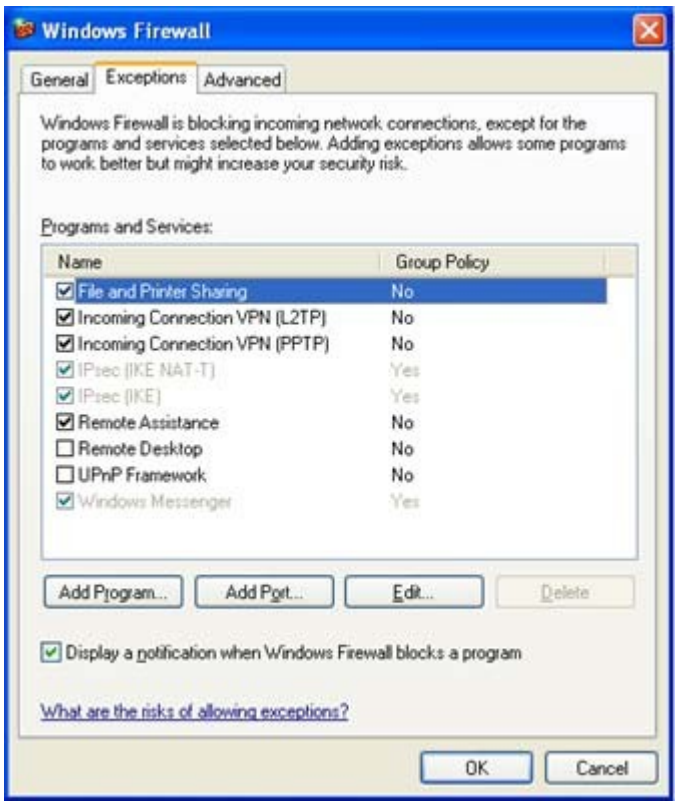
Permitir excepciones a pesar del riesgo

En ocasiones, puede que desee que alguien pueda conectarse a su equipo, a pesar del riesgo; por ejemplo, cuando espere recibir un archivo enviado a través de un programa de mensajería instantánea o cuando participe en un juego con varios jugadores en Internet.

Por ejemplo, si intercambia mensajes instantáneos con alguien que desea enviarle un archivo (como una fotografía), Firewall de Windows le preguntará si desea desbloquear la conexión y permitir que la fotografía llegue a su equipo. O bien, si desea participar en un juego de red con varios amigos en Internet, puede agregar el juego como excepción para que el servidor de seguridad permita que la información del juego llegue al equipo.

Para agregar un programa a la lista de excepciones:

1. Haga clic en **Inicio** y, a continuación, en **Panel de control**.
2. En el Panel de control, haga clic en **Firewall de Windows**.
3. En la ficha **Excepciones**, en **Programas y servicios**, active la casilla de verificación correspondiente al programa o servicio que desee permitir y haga clic en **Aceptar**.



Si el programa (o servicio) que desea permitir no aparece en la lista:

1. Haga clic en **Agregar programa**.
2. En el cuadro de diálogo **Agregar un programa**, haga clic en el programa que desee agregar y, después, haga clic en **Aceptar**. El programa aparecerá, seleccionado, en la ficha **Excepciones**, debajo de **Programas y servicios**.
3. Haga clic en **Aceptar**.

Sugerencia: Si el programa o servicio que desea permitir no se menciona en el cuadro de diálogo Agregar un programa, haga clic en **Examinar**, localice el programa que desea agregar y, a continuación, haga doble clic en él.

Como último recurso, abra un puerto

Si sigue sin encontrar el programa, puede abrir un puerto en su lugar. Un puerto es como una pequeña puerta en el servidor de seguridad que permite que las comunicaciones pasen por ella. Para especificar qué puerto abrir, en la ficha **Excepciones**, haga clic en **Agregar puerto**. (Cuando abra un puerto, recuerde volver a cerrarlo cuando haya terminado de usarlo.)

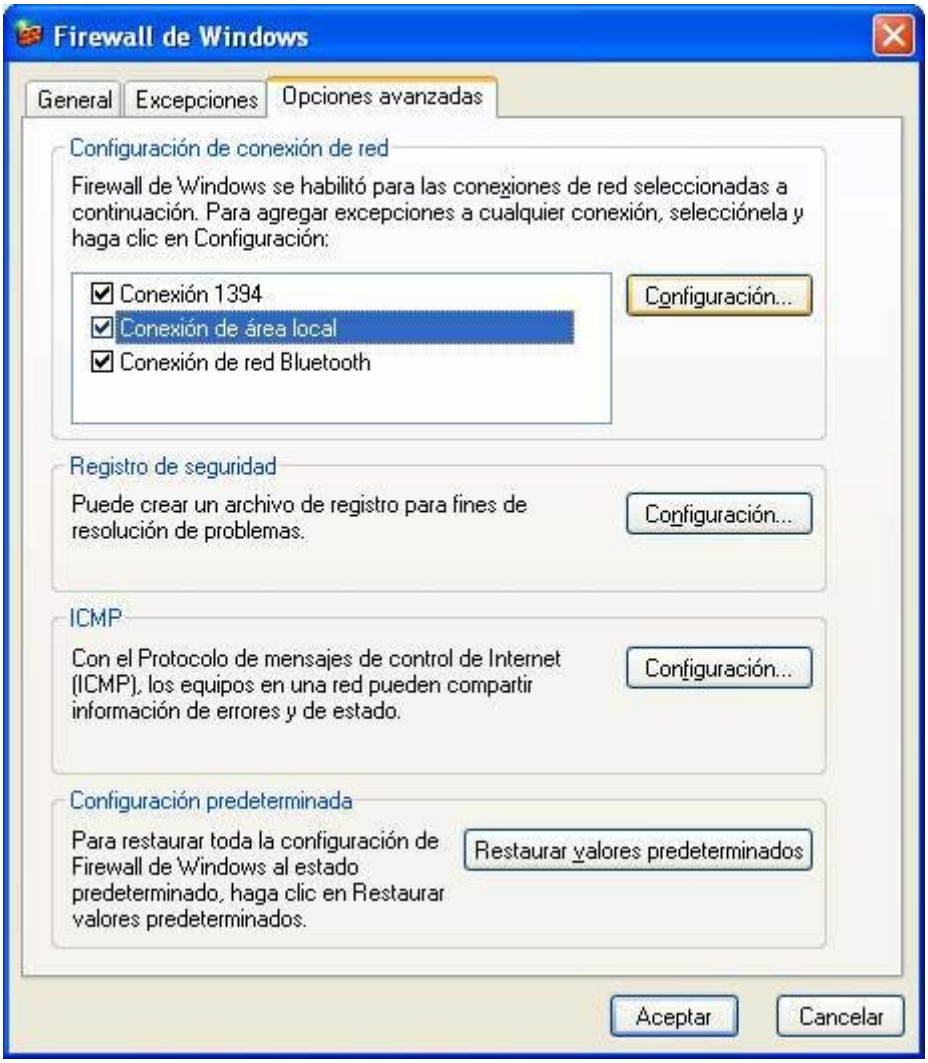
Agregar una excepción es mejor que abrir un puerto porque:

- Es más fácil.
- No necesita saber qué número de puerto usar.
- Es más seguro que abrir un puerto, porque el servidor de seguridad sólo está abierto mientras el programa espera recibir la conexión.

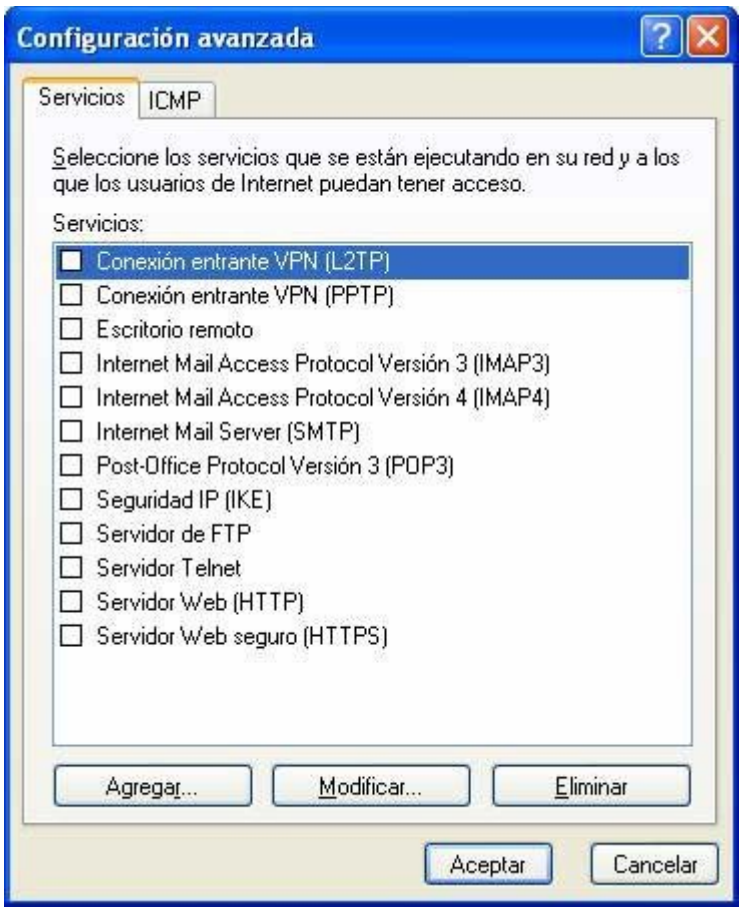
Otras configuraciones

Los usuarios avanzados pueden abrir puertos para conexiones individuales y configurar su ámbito, con el fin de reducir las oportunidades de que los intrusos se conecten a un equipo o una red. Para ello, abra Firewall de Windows, haga clic en la ficha **Opciones avanzadas** y utilice las opciones de configuración de **Configuración de conexión de red**.

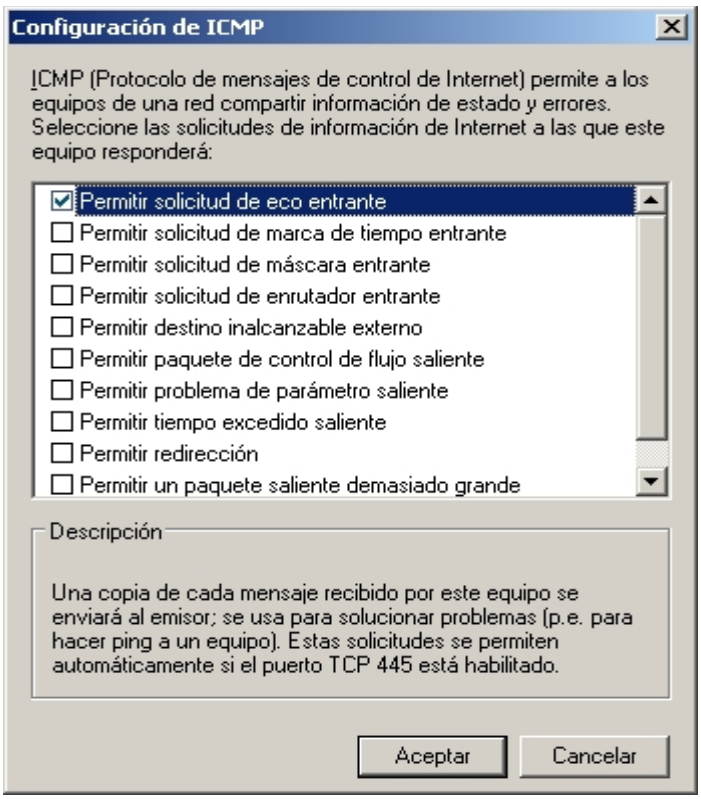
En “Opciones Avanzadas” podemos encontrar otras configuraciones generales del Firewall. Desde este cuadro de diálogo podremos configurar el archivo de log, las conexiones que se verán afectadas por el Firewall (deberían ser todas) y el ICMP (Internet Control Message Protocol).


Firewall de Windows
General
Excepciones
Opciones avanzadas
Configuración de conexión de red
Firewall de Windows se habilitó para las conexiones de red seleccionadas a continuación. Para agregar excepciones a cualquier conexión, selecciónela y haga clic en Configuración:
Conexión 1394
Conexión de área local
Conexión de red Bluetooth
Configuración...
Registro de seguridad
Puede crear un archivo de registro para fines de resolución de problemas.
Configuración...
ICMP
Con el Protocolo de mensajes de control de Internet (ICMP), los equipos en una red pueden compartir información de errores y de estado.
Configuración...
Configuración predeterminada
Para restaurar toda la configuración de Firewall de Windows al estado predeterminado, haga clic en Restaurar valores predeterminados.
Restaurar valores predeterminados
Aceptar
Cancelar

El apartado más interesante es el que afecta a las conexiones, ya que nos permite gestionar todo lo anterior pero esta vez por conexión, lo que en caso de disponer por ejemplo de una tarjeta de red y un módem, nos permitirá gestionar cada uno de ellos de manera diferente. Por último destacar el botón que nos permite restaurar los valores por defecto, extremadamente útil si nos encontramos de pruebas.



Por último, en el apartado de configuración ICMP podemos deshabilitar el que equipos externos nos hagan 'Ping', para saber si nuestra máquina está encendida. Para ello desmarque 'Permitir solicitud de eco entrante', aunque si tenemos activo el servicio SMB en el puerto TCP 445 estas solicitudes se permiten automáticamente.


Configuración de ICMP
ICMP (Protocolo de mensajes de control de Internet) permite a los equipos de una red compartir información de estado y errores. Seleccione las solicitudes de información de Internet a las que este equipo responderá:
Permitir solicitud de eco entrante
Permitir solicitud de marca de tiempo entrante
Permitir solicitud de máscara entrante
Permitir solicitud de enrutador entrante
Permitir destino inalcanzable externo
Permitir paquete de control de flujo saliente
Permitir problema de parámetro saliente
Permitir tiempo excedido saliente
Permitir redirección
Permitir un paquete saliente demasiado grande
Descripción
Una copia de cada mensaje recibido por este equipo se enviará al emisor; se usa para solucionar problemas (p.e. para hacer ping a un equipo). Estas solicitudes se permiten automáticamente si el puerto TCP 445 está habilitado.
Aceptar
Cancelar

Cómo configurar Zone Alarm

Introducción

Los troyanos que pueden instalarse en el mismo y robarnos información. Los escaneos a que nos vemos enfrentados cada vez que navegamos, de quienes buscan una respuesta, o una puerta abierta en nuestra computadora.

Y el mayor peligro: que un troyano esté activo y escuchando.

ZoneAlarm es una utilidad que viene en nuestra ayuda, y es gratuita.

El concepto es simple, ZA nos avisa que aplicación intenta conectarse a Internet, y pone en nuestras manos el permitírselo o no. Muy simple.

Si el Explorer o el Outlook intentan hacerlo cuando Ud. los abre, es lógico. Pero que una misteriosa aplicación llamada xxxx.exe lo intente, no lo es, y menos si nosotros no hemos ejecutado nada que tenga ese nombre. Entonces, simplemente le indicamos a ZA que no le permita conectarse.

ZoneAlarm controla los datos que fluyen de nuestro PC hacia la red y permite a los usuarios decidir qué aplicaciones pueden acceder el Internet.

Y si siente pánico, un botón rojo bloquea todas las conexiones.

ZoneAlarm tal vez no sea la panacea para quienes sientan temor del ataque de un cracker, pero hará más segura su conexión. Y sin dudas, es una herramienta imprescindible, junto a un buen antivirus monitoreando. Y lo es aún más si su conexión a Internet es dedicada (ADSL, cable módem, etc.).

Es fácil de usar, y no necesita conocimientos técnicos como en el caso de otros "firewalls" (cortafuegos). Además, permite que usted coloque un "candado" con clave, para que cuando usted no esté, nadie pueda conectarse a Internet (podrá llamar al proveedor, pero ningún programa podrá comunicarse con la red).

Además, como valor agregado, el ZA impide que un virus del tipo "gusano" o que utilice el lenguaje VBS (Visual Basic Script), como el LoveLetter y tantos otros, se propague a través del correo electrónico, alertándonos de su presencia.

Luego del proceso de instalación, ejecutando el archivo que descargamos de Internet, el ZA quedará en la bandeja de sistema (Systray), o sea, lo veremos presente al lado del reloj.

Cuando nos conectemos a Internet por primera vez luego de ello, el programa interceptará cualquier programa que intente conectarse DESDE nuestra computadora, o cualquier intento de cualquier especie de conexión de un programa o sitio HACIA nuestra computadora.

Simplemente, debemos contestar la pregunta que el ZA nos hará por cada programa que usemos por primera vez (como el navegador, el programa de correo, etc.), si deseamos que se conecte siempre, si lo deseamos hacer solo cuando el ZA nos pregunte, o si no deseamos que se conecte nunca.

Lo ideal es decirle que se conecte siempre a cosas como el navegador y el programa de correo, y lo demás, de acuerdo a su uso. O dejar que nos pregunte cada vez que intente conectarse, y ahí decidir si lo dejamos o no.

Luego de este primer contacto, es muy raro que el ZA nos vuelva a interrumpir con sus preguntas, pero se mantendrá alerta, como fiel guardián.

Configuración de Zone Alarm

Abriendo el ZA con un doble clic sobre su icono, se nos presenta una sencilla configuración, de solo cinco opciones:

- Overview
- Firewall
- Program Control
- Alerts & Logs
- E-Mail Protection

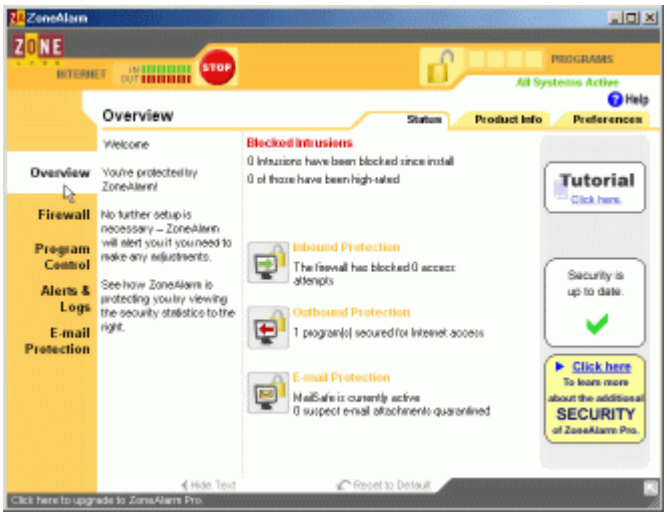
Existen también en la parte superior, un botón rojo con la leyenda STOP y un candado.

El candado, nos deja bloqueado el acceso a Internet de cualquier programa. Incluso podemos agregarle una clave, y su PC podrá llamar al proveedor, pero ningún programa podrá comunicarse con la red.

El botón rojo es una medida de seguridad que nos tranquiliza. Si lo pulsamos, todas las conexiones a la red se paralizan de inmediato.

También vemos al lado del botón de STOP, con la leyenda INTERNET, unas barras que nos muestra el tráfico DE y HACIA nuestro PC (simplemente sirve para ver si hay transferencia de datos activas o no), y al lado del candado los iconos de los programas abiertos capaces de conectarse a Internet (PROGRAMS). Poniendo el cursor sobre ellos veremos su nombre.

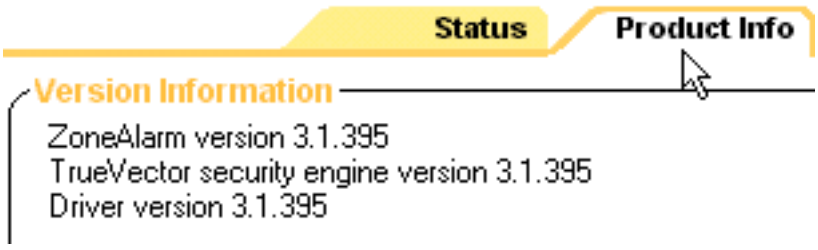
Ésta es la configuración aconsejada para sus principales opciones:



Overview

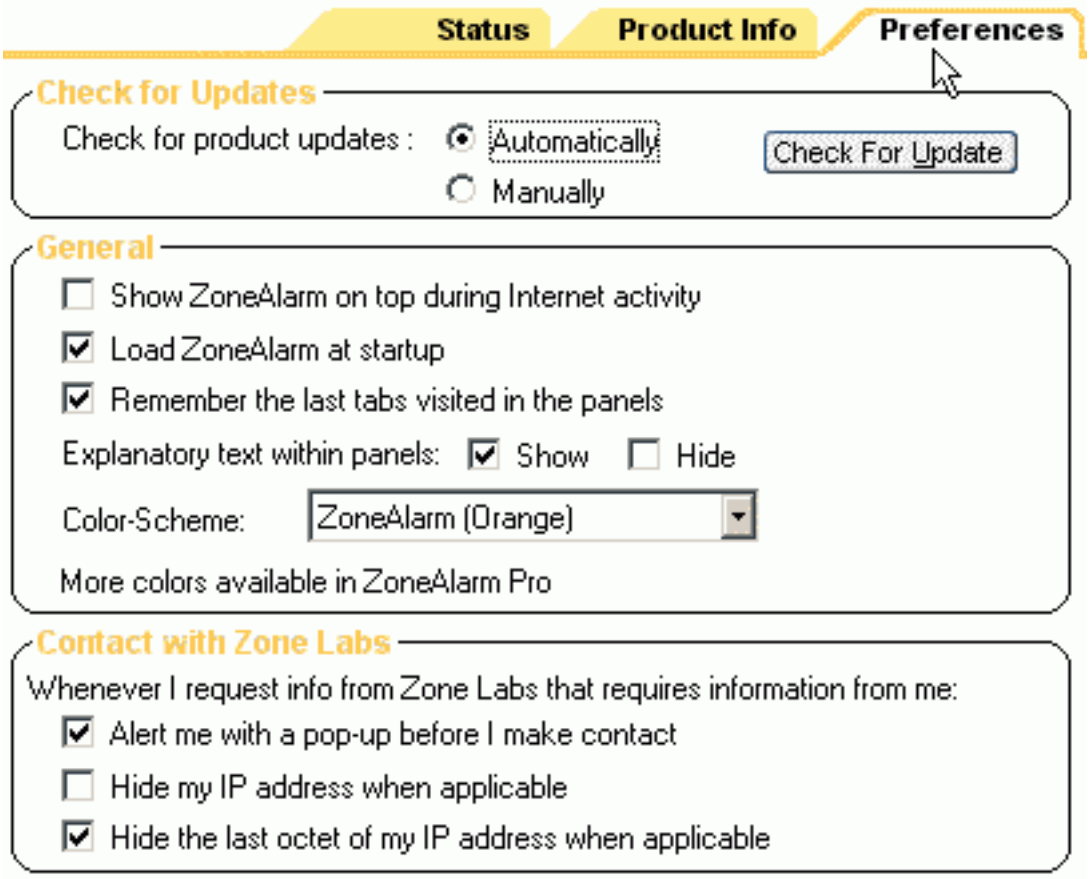
En la lengüeta **STATUS** nos muestra el estado actual del programa y de nuestro sistema. No hay que cambiar nada en principio. Es sólo una pantalla informativa.

PRODUCT INFO sólo nos muestra información de la versión del producto y otros datos relacionados. No hay que cambiar ninguna información importante allí.



En **PREFERENCES**, la información básica durante la instalación no es necesario cambiarla, salvo la opción **"Hide my IP address when applicable"**, que oculta nuestra dirección IP cuando se

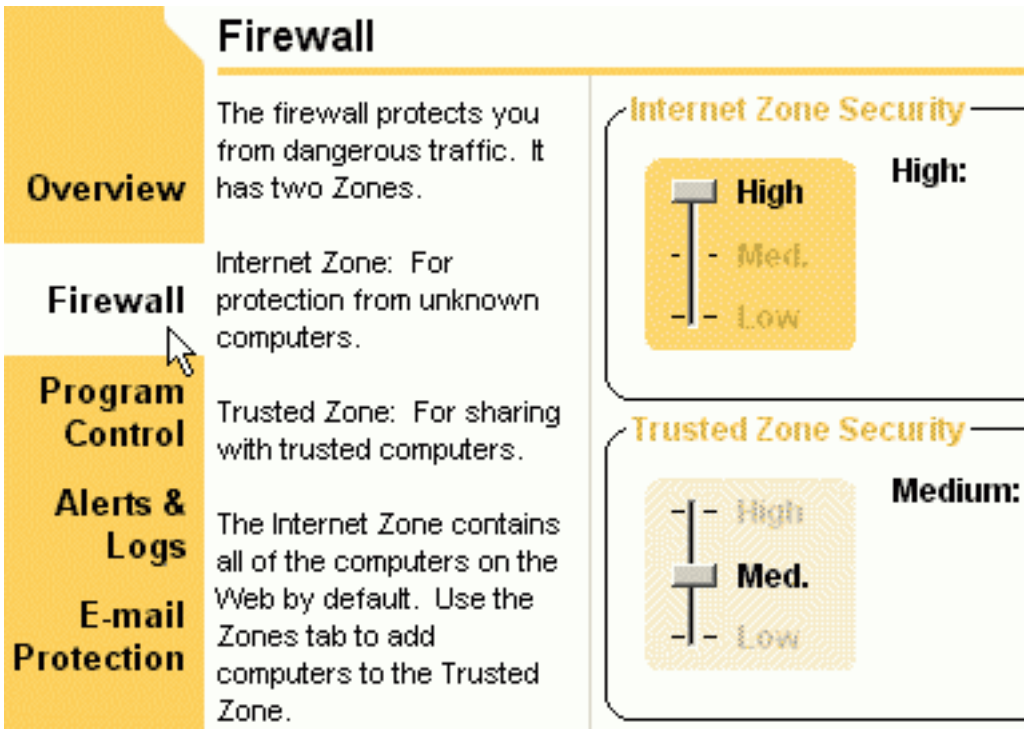
envía un alerta a Zone Labs.


Status
Product Info
Preferences
Check for Updates
Check for product updates :
Automatically
Manually
Check For Update
General
Show ZoneAlarm on top during Internet activity
Load ZoneAlarm at startup
Remember the last tabs visited in the panels
Explanatory text within panels:
Show
Hide
Color-Scheme:
ZoneAlarm (Orange)
More colors available in ZoneAlarm Pro
Contact with Zone Labs
Whenever I request info from Zone Labs that requires information from me:
Alert me with a pop-up before I make contact
Hide my IP address when applicable
Hide the last octet of my IP address when applicable

Firewall

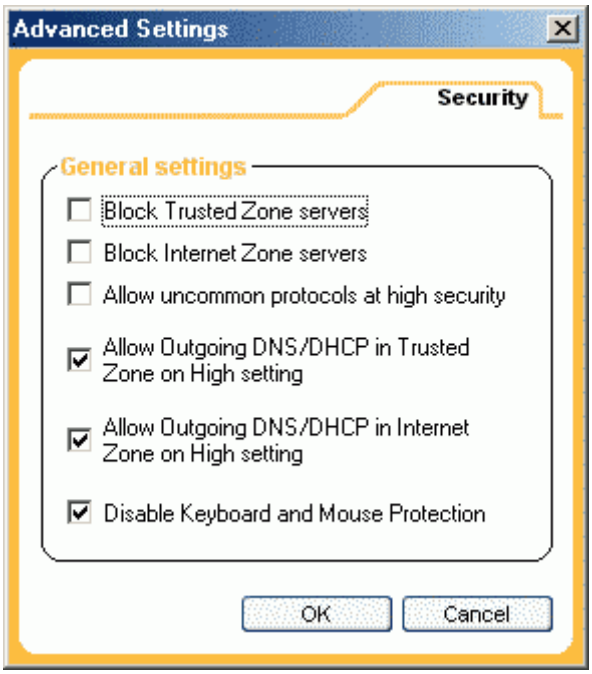
Nos muestra dos pestañas: Main y Zones.

En **Main**, la opción **"Internet Zone Security"** la dejamos en **"High"**, (ver en observaciones más adelante).



La opción **"Trusted Zone Security"** la dejamos en **"Medium"**.

En la misma pantalla, pinchando en el botón **ADVANCED**, en la ventana **Advanced Settings, Security**, las únicas opciones que deben estar marcadas son las tres últimas: **"Allow Outgoing DNS/DHCP in Trusted Zone on High Setting"**, **"Allow Outgoing DNS/DHCP in Internet Zone on High Setting"** y **"Disable Keyboard and Mouse Protection"**.

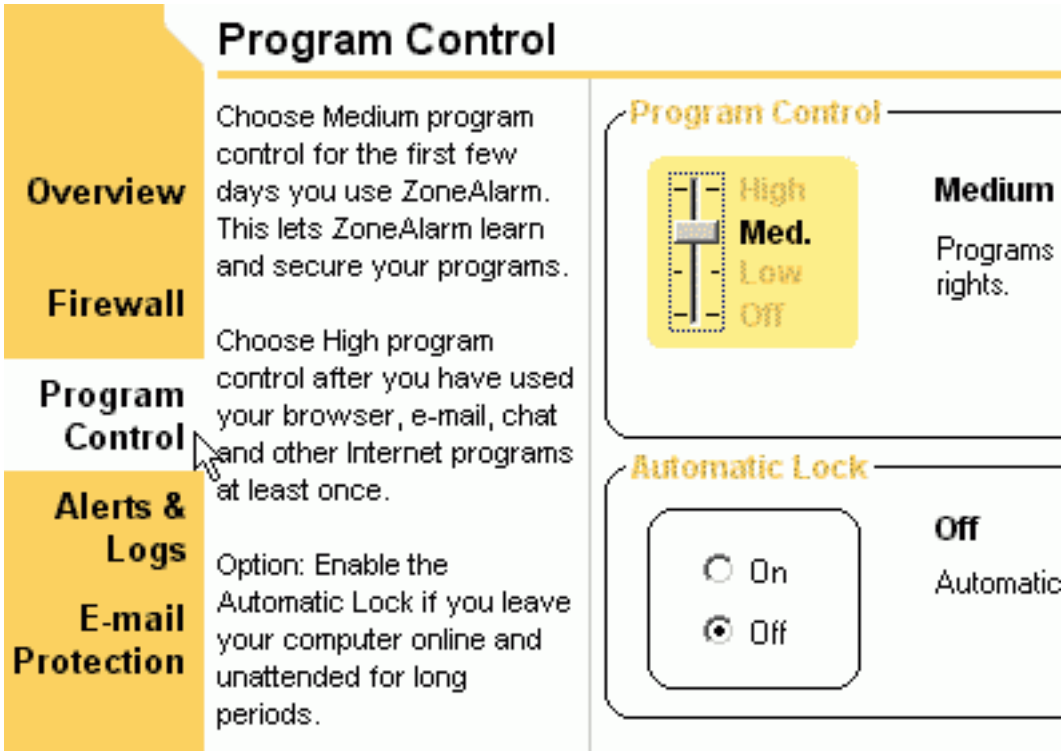

Advanced Settings
Security
General settings
Block Trusted Zone servers
Block Internet Zone servers
Allow uncommon protocols at high security
Allow Outgoing DNS/DHCP in Trusted Zone on High setting
Allow Outgoing DNS/DHCP in Internet Zone on High setting
Disable Keyboard and Mouse Protection
OK
Cancel

No es necesario cambiar nada en la pestaña **Zones** para un usuario único (sin conexión de red).

Program Control

Nos muestra dos pestañas: Main y Programs.

En **Main**, dejamos **"Program Control"** en **Medium** (High no está disponible en la versión gratuita), y **"Automatic Lock"** en **Off**. El botón **Custom** nos permite configurar el Auto-Lock, para bloquear el acceso a Internet cuando se activa el protector de pantallas, etc., y poder controlar esto con contraseña. La idea es impedir que alguien se conecte a Internet cuando no estamos nosotros en la computadora. Sin embargo, tenga en cuenta que la conexión telefónica igualmente se realiza (con su costo correspondiente), sólo que no se puede navegar ni bajar o subir correo, etc. Cualquiera podría intentar conectarse en su ausencia, y si bien no podría hacer nada, la cuenta telefónica seguiría corriendo, téngalo en cuenta. Por lo pronto, olvidémonos de esta opción.



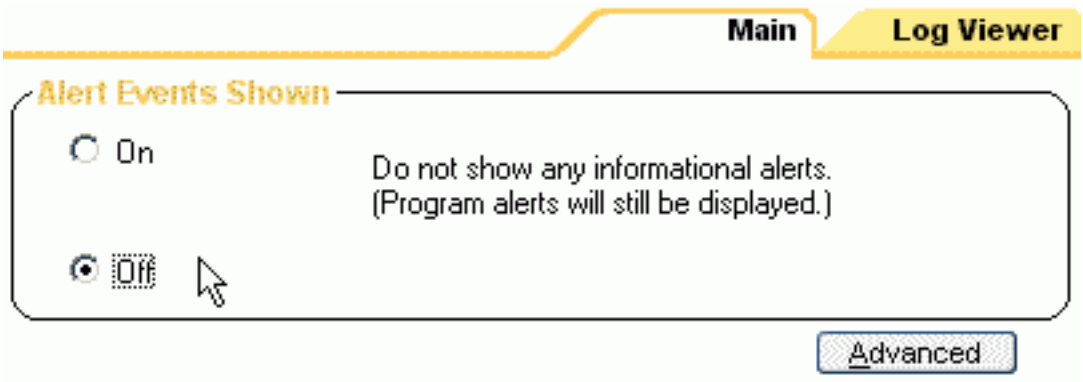
En la lengüeta **Programs** no hacemos nada. Es aquí donde irá quedando la lista de los programas a los que les permitamos ingresar a Internet (Internet Explorer, Outlook Express, GetRight, el antivirus, etc.).

Si alguna vez queremos borrarlo de la lista, o modificar su acción, lo podremos hacer desde aquí.

Alerts & Logs

Nos muestra dos pestañas: Main y Log Viewer.

En **Main**, **"Alert Events Shown"** debe estar en **Off**, de lo contrario nos volveremos paranoicos con el anuncio de cada ping (paquete de control), y otras lindezas que suelen mandarnos algunos sitios, además de todas las posibles intrusiones externas. Pero es importante tener en cuenta, que no ver las alertas, no significa que estemos desprotegidos, sino que ZA nos mantendrá protegidos sin molestarnos.



En la pestaña **Log Viewer**, veremos la lista de posibles intrusiones, etc. Tiene sólo valor documental y rara vez debemos apelar a examinar su contenido.

E-Mail Protection

Las opciones son **On y Off** para **"Basic MailSafe"**. La dejamos en **ON**. En la versión gratuita del ZA, esto nos protege de la ejecución de adjuntos con extensión **.VBS** solamente.

Observaciones

No existen problemas destacables en mantener la configuración de **"Internet Zone Security"** (en **FIREWALL**) en máxima seguridad (High), es más, es aconsejable mantener esta opción en **"High"**. De cualquier modo, podemos perfectamente "bajar" esta configuración a **"Medium"**, y luego subirla a **"High"** si tuviéramos alguna dificultad con la conexión a algún sitio en particular. Y todo ello "en caliente", o sea que los cambios son tomados en el momento.

La opción **HIGH** vuelve invisible a nuestro PC ante los ojos del mundo exterior, en cambio la opción **MEDIUM**, deja el PC visible, pero igualmente SEGURO.

Existe una página web: http://grc.com/default.htm (seleccione **"Shields Up!!!"** y luego **"Test My Shields!"** y **"Probe My Ports!"**), que nos permite revisar la seguridad de los puertos de nuestro ordenador. Podemos probarlo con el ZA activo.

Con la opción **HIGH**, el resultado va a ser: **STEALTH!** (ocultos, los puertos peligrosos existen, pero están invisibles para cualquier escaneo de puertos desde el exterior)

Con la opción **MEDIUM**, el resultado es: la mayoría **STEALTH!**, y los puertos 79 (Finger), 80 (HTTP), 110 (POP3), y 143 (IMAP), **CLOSED** (cerrados), lo que significa que el PC es reconocida -"está ahí" para quien escanea, y para los sitios que necesitan esto para identificarnos como "vivos",

para permitirnos bajar archivos, por ejemplo-, pero lo más importante, están CERRADOS, lo que significa que nadie podrá acceder por ellos a nuestro PC.

Recordemos que debemos sumar al ZA un buen antivirus que nos proteja de troyanos. Aún cuando el ZA nos avisa si un programa de nuestro PC intenta conectarse a Internet (cosa que debemos permitir en el caso del Internet Explorer, Outlook Express, etc.), no sería conveniente dejar que lo haga un programa que no conocemos. Un antivirus complementará esta acción, identificando al troyano o gusano, eliminándolo si lo fuera.

Como siempre, debemos tener muy claro que la principal barrera seguiremos siendo nosotros, no ejecutando programas sin revisarlos antes con un antivirus al día, no abriendo adjuntos no solicitados que recibamos por e-mail, y aún en el caso de los solicitados, revisándolos en una carpeta con uno o dos antivirus al día antes de ejecutarlos.

Conclusiones

El Firewall proporciona la mayoria de las herramientas para complementar su seguridad en una red (mediante la imposición de políticas de seguridad), en el acceso a los recursos de la red y hacia la red externa. Es importante establecer una monitorización constante que nos permitirá detectar un posible intruso y así proteger la información. Es prácticamente imposible que protejamos al 100 % nuestra red de crakers cuando dentro de nuestra organización puede existir personal traidor y que puede sabotear nuestro sistema.

Bibliografía

1. **Manual de Firewalls**. Marcus Goncalves. Editorial McGraw-Hill.
2. **Cortafuegos (informática) - Wikipedia, la enciclopedia libre**. http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)
3. **Radiográfica Costarricense S.A.** http://www.racsa.co.cr/consejos_navegacion/proteccion/firewalls/index.html
4. **Beneficios de un firewall en Internet.** http://www.lanrouter.com/content/view/38/71/
5. **Limitaciones de un firewall.** http://www.lanrouter.com/content/view/39/72/
6. **Firewall, la muralla defensiva de un PC.** http://www.terra.es/tecnologia/articulo/html/tec10589.htm
7. **Diferentes tipos de intrusiones y ataques.** http://www.terra.es/tecnologia/articulo/html/tec10590.htm
8. **Firewalls.** http://html.rincondelvago.com/firewalls.html
9. **The Differences and Features of Hardware & Software Firewalls.** http://www.webopedia.com/DidYouKnow/Hardware_Software/2004/firewall_types.asp
10. **Configuración de un firewall en Linux con iptables - El Rincón del Programador.** http://www.elrincondelprogramador.com/default.asp?pag=articulos/leer.asp&id=14
11. **Windows Firewall.** http://www.uned.es/csi/sistemas/secure/seguridad/docs/xp-firewall.htm
12. **Cómo configurar Zone Alarm.** http://www.vsantivirus.com/za.htm
13. **Seguridad Firewall: Firewall por hardware o software.** http://www.dric.com.mx/seguridad/firewall/firewall1.php?cat=4&scat=4